FISH.
FISH & RICHARDSON

Fish & Richardson P.C.
222 Delaware Avenue
17th Floor
P.O. Box 1114
Wilmington, DE 19899-1114

302 652 5070 main
302 652 0607 fax

Susan E. Morrison
Principal
morrison@fr.com
302 778 8434 direct

VIA: ECF/E-MAIL

November 17, 2021

The Honorable Sherry R. Fallon
J. Caleb Boggs Federal Building
844 N. King Street
Unit 14
Room 6100
Wilmington, DE 19801-3555

Dear Judge Fallon:

Defendant McAfee Corp. ("McAfee") respectfully requests an order compelling Plaintiff Kajeet, Inc. ("Kajeet") to: (1) amend its infringement contentions to properly disclose its theory of infringement for U.S. Pat. No. 8,667,559 ("the '559 patent") and (2) respond to McAfee's Interrogatory No. 1, which requests source code citations supporting Kajeet's theory of infringement. This order is required because, earlier in the case, McAfee challenged the specificity and viability of Kajeet's theory via both a Motion to Dismiss and a Motion for Rule 11 Sanctions. The Court denied the Rule 11 motion as moot, but indicated a willingness to consider a renewed Rule 11 motion "should it become apparent later after sufficient discovery that Kajeet cannot reasonably maintain its assertions of infringement." Oct. 8, 2021 Hr'g Tr. 21:22-23:1. This ruling came after Kajeet expressly represented that it would disclose a specific theory in its infringement contentions—including specifically source code citations:

> Well, certainly we will provide specific references to evidence and documents, and later source code once we receive that source code. So we will certainly be more specific than that in our contentions and we have been. So we served contentions on them addressing specific documents, excerpts from documents and those are the things that McAfee's counsel claims need to be in the complaint, but we definitely will be more specific in our contentions.

Oct. 8, 2021 Hr'g Tr. 10:3-11. McAfee has made its source code available for inspection since July 2, 2021 (fully five months ago), and Kajeet has inspected the code multiple times. To date, however, Kajeet has failed to provide the promised "specific references" to source code.

Background

McAfee's Safe Family product, which Kajeet accuses of infringing claims 1 and 27 of the '559 patent, is a parental controls application that lets a parent set limits on the usage of their child's device. However, no product can infringe Kajeet's patent, including specifically McAfee's Safe Family application, unless it controls the operation of a device using a set of "policies" that are ***remotely stored*** on a server—and ***not accessed locally*** on the controlled device. Using claim 1 as an example, the claimed system requires that when a controlled device seeks to communicate

over a network, (1) a remote server makes a decision (enabling or denying the requested communication) based on a policy stored at that server (*see, e.g.*, D.I. 1 at Ex. A, '559 Pat. at cl. 1 ("the decision being based on one or more policies that are stored at the server")); (2) the remote server provides to the controlled device a response indicative of the decision in real time (*id.* ("receive in real-time from the server a response indicative of a decision granting or denying the request")); and (3) the policy that determines whether to grant or deny a request is not accessed by the controlled device (*id.* ("the requested communication being enabled or disabled ***without accessing*** the one or more policies by the computing device")).

These limitations are nontrivial to the purported validity of the alleged invention. Kajeet repeatedly references this enforcement of remotely stored policies when describing the alleged benefits of the claimed invention and how it differs from the prior art. *See, e.g.,* D.I. 14, Am. Compl. ¶ 19 ("Application of use decisions based upon ***a policy stored remote from the controlled computing device*** represented an unconventional scheme that was neither well known nor routine for addressing a newly emerging problem in society.")(emphasis added); *see also* ¶¶ 36, 37, 40. Kajeet also relied on the remote storage of policies to survive a Section 101 challenge to patentability in this Court. *See, e.g., Kajeet, Inc. v. Nortonlifelock Inc.*, C-A No. 20-1339 Dkt. No. 19 (Dec. 23, 2020) ("By virtue of storing policies remotely from the controlled device, they are inaccessible to the controlled device for manipulation or deletion, thereby improving system effectiveness."); *id.* at 3 ("Kajeet addressed these shortcomings by storing usage policies remotely from the communication device(s).").

Kajeet's infringement contentions, however, wholly ignore the requirement that "the requested communication [is] enabled or disabled without accessing the one or more policies by the computing device." D.I. 1 at Ex. A, '559 Pat. at cl. 1. The reason for this glaring hole in Kajeet's infringement contentions is that McAfee's Safe Family product simply does not do what the claims require. Safe Family instead caches all of the accused "policy" information locally at each device. McAfee demonstrated this to Kajeet before its infringement contentions were due, and even identified a variety of tests that Kajeet could itself perform to confirm Safe Family's operations. D.I. 35 at 10, 13. McAfee further produced all of the source code for the accused products to allow Kajeet to verify the Safe Family's operation. Because Kajeet's infringement contentions remained inadequate, McAfee served an interrogatory seeking source code support for Kajeet's infringement theory. *See* Exhibit A at Interrogatory No. 1 (September 15, 2021); D.I. 45. Kajeet refused to respond to that interrogatory. *See* Exhibit B; D.I. 55.

Kajeet Must Disclose its Infringement Theory

Claim 1 requires that communication are enabled or disabled in real time based on a policy stored on server without accessing the one or more policies by the computing device. Kajeet ***could*** have set forth a theory in a number of different ways ***if*** one was available. For instance, Kajeet could use freely available network analysis tools to observe the timing and type of communications between a controlled device and a server to determine whether the controlled device was receiving real time decisions over a network. Alternatively, Kajeet could have observed the operation of a controlled device that was not connected to a network to determine

whether the device needed to be connected to a remote server to operate. Or, as yet another option, Kajeet could cite to source code that McAfee produced in this case. Kajeet did none of the above, even after McAfee brought this issue to Kajeet's attention. D.I. 17 (McAfee's Motion to Dismiss), 18 (McAfee's Opening Brief in Support of its Motion to Dismiss) (identifying defects in Kajeet's infringement theory); D.I. 34 (Motion for Sanctions Under Rule 11), 35 (Opening Brief in Support of Motion for Sanctions Under Rule 11) (similar).

Instead, for the last limitation of claim 1, Kajeet provides only a generic statement that Safe Family lets a parent set "policies" using a parent version of the application. That statement is irrelevant to the issue underlying that limitation: namely, whether McAfee's products access "policy" information locally in contravention of the '559 claim requirements. *See* Ex. E, Kajeet's Infringement Contentions at 22 (Aug. 19, 2021). Thus, from Kajeet's contentions, McAfee is not able to prepare its defenses. For example, although Kajeet opposed McAfee's Motion for Rule 11 sanctions, McAfee cannot determine if the basis for Kajeet's opposition is how the product operates, or the scope of the claims. Relatedly, McAfee cannot determine the claim scope it should be applying for its affirmative defense of invalidity.

Importantly, Kajeet interprets its contentions the same way. When responding to McAfee's complaint on this issue, Kajeet describes that its contentions concern "policies . . . set by parents and stored on McAfee's servers," but failed to acknowledge the nature of McAfee's complaint, which relates to the negative limitation in the claim:

> Kajeet's PICs demonstrate that policies upon which decisions are based are set by parents and stored on McAfee's servers. Kajeet's PICs also show that decisions based on these policies are communicated to a child's device and enforced to effect control over use of the child device.

See Exhibit C (Email from Richard Wojcio, Jr. to Aamir Kazi on October 19, 2021). Kajeet even promises forthcoming supplements. *Id.* ("Going forward we expect that Kajeet's infringement contentions will be supplemented to include additional, non-public information about the Safe Family product that will be produced in discovery."). But there is no reason that Kajeet should not provide that supplement now, as fairness and efficiency dictates.

Kajeet does not need any further discovery to specify its theory. While Kajeet vaguely contends that McAfee did not timely produce certain source code (McAfee disagrees with that contention), Kajeet does not dispute that it has access to all relevant source code today—and has had such access for months. And regardless, in opposing McAfee's motion for sanctions on this very issue, Kajeet represented to the Court that it had source code and testing evidence to substantiate its infringement theory. D.I. 40 at 19. Kajeet even submitted an *in camera* expert declaration to the Court in camera setting forth this alleged theory. Thus, Kajeet contends it has an infringement theory—so it must disclose that theory of infringement in this case now. *Kinglite Holdings Inc. v. Micro-Star International Co.,* No. CV 14-03009 JVS (PJWx), 2016 WL 6762573, at *2 (C.D. Cal. June 15, 2016) (ordering patentee to serve contentions with specific reference or "pinpoint citations to source code" where the patentee was able to do so); *Am. Video*

Graphics, L.P. v. Elec. Arts, Inc., 359 F. Supp. 2d 558, 561 (E.D. Tex. 2005) (plaintiff must supplement its initial charts with "specific references to the source code" within thirty days of defendant providing plaintiff with the source code)."

Kajeet Must Respond to McAfee's Interrogatory No. 1.

In still further efforts to ascertain Kajeet's infringement theory, McAfee served an interrogatory seeking source code citations supporting Kajeet's infringement contentions. Kajeet's response to this interrogatory includes only four pages of objections. Kajeet did not identify which specific objection(s) Kajeet was relying upon here, but none justify refusing to provide any response.

First, Kajeet's objections to the scope of the interrogatory, if credited, still require a response to the part that Kajeet finds to be unobjectionable. *Jordan v. Mirra*, No. 1:14-CV-01485-GAM, 2019 WL 2127788, at *19 (D. Del. Feb. 27, 2019), *report and recommendation adopted*, No. CV 14-1485, 2019 WL 2121346 (D. Del. May 15, 2019) (requiring party to "explicitly respond to all portions of the interrogatories"). Kajeet did not do so.

Second, Kajeet's objections to the timing of this interrogatory are not supported by the law of this District. *Integra LifeSciences Corp. v. HyperBranch Med. Tech., Inc., 223 F. Supp. 3d 202, 206* (D. Del. 2016) (requiring party to answer contention interrogatory during discovery). Here in particular, Kajeet's response to Interrogatory No. 1 is necessary to understand the Rule 11 basis for Kajeet's allegations of infringement. *Jordan v. Mirra,* 2019 WL 2127788, at *17–18 (D. Del. Feb. 27, 2019), report and recommendation adopted, No. CV 14-1485, 2019 WL 2121346 (D. Del. May 15, 2019) (finding it appropriate to require early answers to contention interrogatories where "there is good reason to believe that answers to [] well-tailored questions will contribute meaningfully to clarifying the issues in the case, narrowing the scope of the dispute, or setting up early settlement discussion, or that such answers are likely to expose a substantial basis for a motion under [Federal Rule of Civil Procedure] 11"). Indeed, in defending itself against Rule 11 allegations, Kajeet represented that it would be providing source code citations. Hearing Tr. at 10:3-11 ("Well, certainly we will provide specific references to evidence and documents, and later source code once we receive that source code.")

The remainder of Kajeet's objections are factually incorrect and irrelevant. McAfee previously agreed to provide source code citations supporting its noninfringement positions (in addition to the narrative discussion and the testing evidence McAfee has already provided) if Kajeet provides source code citations to support its infringement theory. *See* Exhibit D (Email from Aamir Kazi to Corby Vowell on September 3, 2021). Kajeet refuses to do so. With respect to Kajeet's access to McAfee's source code, McAfee timely made all source code available and provided all print copies that were compliant with the agreed upon protective order. And regardless, Kajeet does not dispute that it has access to McAfee's source code today.

In sum, despite Kajeet representing to McAfee and to the Court that it would supplement its infringement contentions, including references to source code, Kajeet now refuses to do so. For the foregoing reasons, the Court should grant McAfee's motion to compel.

Respectfully submitted,

/s/ Susan E. Morrison

Susan E. Morrison

cc: All counsel of record (via ECF/Electronic mail)